

24 MAG 1398

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All
Content and Other Information
Associated with the iCloud Account
Associated with [REDACTED] bk.ru,
Maintained at Premises Controlled by
Apple Inc., USAO Reference No.
2021R00778

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

**Agent Affidavit in Support of Application for a Search Warrant
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

[REDACTED] Special Agent, Federal Bureau of Investigation, being duly sworn, deposes
and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since 2019. I am currently assigned to a public corruption squad of the New York Field Office, where, among other things, I investigate crimes involving illegal campaign contributions, theft of federal funds, and bribery. Through my training and experience, I also have become familiar with some of the ways in which individuals use smart phones and electronic communications, including social media, email, and electronic messages, in furtherance of their crimes, and have participated in the execution of search warrants involving electronic evidence.

B. The Provider, the Subject Account and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the iCloud accounts associated

with [REDACTED]bk.ru (the “[REDACTED] iCloud Account” or the “Subject Account”), maintained and controlled by Apple Inc. (the “Provider”), headquartered at 1 Infinite Loop, Cupertino, California 95014. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Account contains evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same), and (iv) 18 U.S.C. § 1956 (money laundering and conspiracy to commit money laundering) (collectively, the “Subject Offenses”). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

4. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

5. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

6. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as AOL). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

7. Apple captures information associated with the creation and use of an Apple ID.

During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

8. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

9. Apple also maintains information about the devices associated with an Apple ID.

When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

10. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud Drive. Some of this data is stored on Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

11. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

12. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

13. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

14. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

15. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

16. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

D. Jurisdiction and Authority to Issue Warrant

17. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

18. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

19. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Subject Offenses

20. Since in or about August 2021, the FBI and the Office of the United States Attorney for the Southern District of New York have been investigating the receipt of so-called “straw” donations by the 2021 and 2025 New York City mayoral campaigns of Eric Adams (the “2021 Adams Campaign,” the “2025 Adams Campaign,” and, collectively, the “Adams Campaigns”), including certain straw donations that were funded by and/or made at the direction of foreign government officials and other foreign persons.¹

21. As part of this investigation, law enforcement has obtained various warrants for electronic evidence, including but not limited to the following:

a. On December 2, 2022, the Honorable Stewart D. Aaron, United States Magistrate Judge for the Southern District of New York, issued a warrant permitting a search of an iCloud account used by Adams. The warrant and supporting affidavit are attached hereto as Exhibit A and incorporated by reference herein.

¹ A straw, or “conduit,” donation occurs when a donation to a political campaign is made in the name of one donor, but the funds in question in fact belong to a different person.

b. On November 5, 2023, the Honorable Gary Stein, United States Magistrate Judge for the Southern District of New York, issued a warrant permitting the seizure and search of electronic devices in Adams's possession (the "November 5 Warrant"). The November 5 Warrant and supporting affidavit are attached hereto as Exhibit B and incorporated by reference herein.²

The Adams Campaign Seeks Matching Funds from New York City

22. I understand, based on my review of publicly available information, that:

a. The Adams Campaigns accepted matching funds from the New York City Campaign Finance Board throughout a significant part of its campaign ("Matching Funds"), meaning that the Adams Campaigns received funds from the New York City government as a result of donations the Adams Campaigns received from private donors that were eligible for matching funds.³

b. Under New York City law, the Adams Campaigns were eligible to receive \$2,000 in Matching Funds, and no more than \$2,000 in Matching Funds, for each donation of \$250 from an individual donor who resides within New York City, subject to certain exceptions not relevant here. If an individual donated more than \$250, any amount in excess of \$250 would not be eligible for matching funds.⁴

² We are continuing to investigate the conversation described in Paragraph 13 of Exhibit B and are not presently asking the Court to rely on that conversation in making its probable cause determination.

³ See, e.g., <https://ny1.com/nyc/all-boroughs/news/2021/10/08/eric-adams-is-taking-a-rare-step--turning-down-campaign-cash> (reporting on the Adams Campaign's prior acceptance of matching funds and decision to turn down some matching funds as of October 7, 2021); https://www.nycfb.info/VSAppls/CandidateSummary.aspx?as_cand_id=1545&as_election_cycle=2021&cand_name=Adams%2C+Eric+L&office=Mayor&report=summ (New York City Campaign Finance Board's report detailing total public funds disbursed to Adams Campaign).

⁴ See <https://www.nycfb.info/candidate-services/join/>.

- c. New York City receives in excess of \$10,000 per year in federal funding.⁵

The Adams Campaigns Receive Straw Donations

23. As detailed more fully in the attached affidavits, this investigation has revealed, in substance an in part, the following:

a. On or about May 7, 2021, employees of [REDACTED] (“[REDACTED]”) a construction company that operates in New York City, made donations to the 2021 Adams Campaign in approximately the same amount as monies paid to each of the employees by [REDACTED] on April 28, 2021.⁶ (*See, e.g.*, Ex. A ¶¶ 10-12).

b. Many of [REDACTED] employees are of Turkish origin.⁷ (*See, e.g.*, Ex. A ¶ 8).

c. The Adams Campaigns cultivated a relationship with Turkey’s New York Consul General, as well as the broader Turkish community, beginning at least in 2018. (*See, e.g.*, Ex. A ¶ 19; Ex. A of Ex. B ¶¶ 16, 19).

d. Turkey’s Consul General in New York was involved in fundraising for the Adams Campaigns, including the arrangement of the fundraiser where the [REDACTED] straw donations were made, and communicated about fundraising with members of Adams’s staff.⁸ (*See, e.g.*, Ex. A ¶ 19; Ex. A of Ex. B ¶¶ 12(a), 12(b), 13, 16).

⁵ *See, e.g.*, https://comptroller.nyc.gov/wp-content/uploads/2016/11/Federal_Budget_Vulnerabilities_Memo.pdf.

⁶ Out of eleven donations from [REDACTED] employees made at the fundraiser, the co-owner of [REDACTED] who organized the fundraiser did not receive a [REDACTED] reimbursement check, one donor received \$50 more from [REDACTED] than the donor donated to the Adams Campaign, and one [REDACTED] employee’s wife donated, while the employee himself received the [REDACTED] reimbursement check.

⁷ Certain earlier affidavits in this investigation stated that [REDACTED] was affiliated with a larger Turkish corporation. Law enforcement has since interviewed several [REDACTED] employees who have stated, in substance and in part, that although [REDACTED] was started by personnel formerly employed by that larger Turkish corporation, the two entities have no formal connection.

⁸ Certain earlier affidavits in this investigation described [REDACTED] and [REDACTED] as staff of the Adams Campaigns. Counsel for Adams has since told the Government that, at least

e. Turkish national [REDACTED] was involved in fundraising for the Adams Campaigns and attempted, in agreement with Adams Campaign staff, to donate funds from Turkish nationals to the Adams Campaigns and communicated about fundraising with members of Adams Campaign staff.⁹ (*See, e.g.*, Ex. A of Ex. B ¶¶ 19-24).

f. Adams communicated with members of his staff about fundraising in the Turkish community and the potential provision of benefits to the Consul General. (*See, e.g.*, Ex. A of Ex. B ¶¶ 16(i), 16(j)).

g. Adams and members of his staff intervened in at least one matter within the purview of the New York City government to obtain favorable action for the Consul General; specifically, obtaining a Temporary Certificate of Occupancy (“TCO”) for the official opening of a building associated with the Turkish Consulate in New York in time for a visit by Turkey’s president in 2021. (*See, e.g.*, Ex. A of Ex. B ¶¶ 25-29).

24. Adams and others associated with him received various benefits from persons affiliated with the Consul General, including travel to Turkey via [REDACTED] that was provided at no cost in some instances, and reduced cost in others. (*See, e.g.*, Ex. A of Ex. B ¶ 17).

with respect to the 2021 Adams Campaign, [REDACTED] was a volunteer and [REDACTED] was a volunteer before becoming an employee of the Campaign. As used herein, “Adams’s staff” is an inclusive term referring to persons who have worked for Adams (whether as Brooklyn Borough President or Mayor) and/or the Adams Campaigns.

⁹ In addition to other such donations, [REDACTED] assisted in coordinating straw donations from employees of [REDACTED] (“[REDACTED] a Washington, D.C.-based university partnered with a Turkish university named [REDACTED]”). Records maintained by the New York City Campaign Finance Board indicate that on September 27, 2021, five employees of [REDACTED] donated \$2,000 each to the 2021 Adams Campaign. According to public reporting, the 2021 Adams Campaign returned the [REDACTED] donations approximately 17 days later, claiming that “[t]he campaign had raised more money than it could spend,” but the article notes that “campaign records show [the 2021 Adams Campaign] accepted and did not return other contributions in the weeks that followed.” *See* <https://www.thecity.nyc/2023/11/03/fbi-probe-eric-adams-campaign-turkey>.

██████████ *is Connected to both Adams and the Government of Uzbekistan*

25. ██████████ is the founder of the Silk Road Foundation, an organization that purports to support families that have migrated to the United States from Central Asia.¹⁰ Based on my review of records from a law enforcement database, I know that ██████████ is a dual American and Uzbek citizen.

26. ██████████ social media indicates that he works with the Government of Uzbekistan to promote Uzbek causes in the United States. For instance, in substance and in part:

a. In or about the summer of 2023, ██████████ posted a picture on social media with a caption that he was at a “dinner with Uzbek officials” where “we discussed the rich heritage of Uzbekistan and how we can together help promote it in the United States.”

b. Also in or about the summer of 2023, ██████████ posted a picture with a caption stating: “We met with the Minister of Natural Resources of Uzbekistan, Mr. ██████████ today”

c. In or about late 2023, ██████████ posted a picture of a watch in a ceremonial case. The caption says “Thank you Mr. President” and tags the account of the President of Uzbekistan.

27. Based on my review of records from a phone company for a phone number ending in 7009 (the “██████████ Phone”), I have learned that the phone is subscribed to ██████████ and that between on or about April 9, 2023, and on or about January 17, 2024, the ██████████ Phone had approximately 292 communications with a phone with a number ending in 0440. Based on my review of records from a law enforcement database, I know that the 0440 number is used by a member of the Uzbekistan Permanent Mission to the United Nations.

¹⁰ See <https://www.brooklynbp.nyc.gov/nearly-200-brooklynites-join-brooklyn-borough-president-antonio-reynoso-for-second-annual-ramadan-iftar-at-borough-hall/>.

28. Based on my review of social media posts, I have also learned that [REDACTED] attends official events with Adams. For instance, in substance and in part:

a. In or about April 2023, [REDACTED] posted two photos on social media. One is captioned: “Attended a fantastic iftar event hosted by Mayor Eric Adams yesterday! It was incredible!” The other is a photo of [REDACTED] with Adams, captioned “With the Mayor of NYC Eric L. Adams #nycmayor.”

b. On or about July 18, 2023, an organization named “Makonim USA” posted on Facebook describing a “HISTORIC EVENT”: “the 1st ever Uzbek community roundtable with Mayor Eric Adams took place inside City Hall. . . . Very proud of Silk Road Foundation and [REDACTED] for being the leaders who really care about their community and working hard to bring resources to their people.”

c. Also in approximately July 2023, [REDACTED] posted a photo of himself with Adams. The photo was captioned “Dear Gosht team, congratulations on the grand opening! Wishing you success, growth, and prosperity!!!” The post also stated that it was located in Brooklyn, New York. According to open-source information, there is a halal restaurant named Gosht in Brooklyn.

d. In or about September 2023, [REDACTED] posted a photo of himself with Adams. The photo was captioned “Happy Uzbekistan Independence Day! . . . Mayor Eric Adams made history by being the first to raise the Uzbek flag on Wall Street! A proud moment for NYC’s vibrant Uzbek community.” Based on my review of public posts for an account on X.com (formerly Twitter.com) belonging to Adams, I know that Adams also posted pictures from a flag raising on Uzbekistan Independence Day.”¹¹

¹¹ See <https://twitter.com/NYCMayor/status/1698035304978927860>.

29. Based on my review of phone records for the [REDACTED] Phone, I have learned the following:

- a. In or about 2023, [REDACTED] had approximately one call with a phone number ending in 3179, which is the number of Adams' personal cellphone (*see* Ex. B ¶ 15).
- b. In or about October 2023, [REDACTED] had approximately two calls with a phone number ending in 2780. Based on my participation in the investigation, including my review of electronic devices belonging to [REDACTED] a fundraiser for the Adams Campaigns (*see* Ex. A at ¶ 19, Ex. B at ¶¶ 8, 10)—the 2780 number is used by [REDACTED]
- c. Between in or about January 2023 and in or about January 2024, [REDACTED] had approximately fifty-five calls with a phone number ending in 0470. Based on my review of records from a law enforcement database, I have learned that the 0470 number is used by [REDACTED] the Commissioner for the New York City Office of Community Affairs.

[REDACTED] *Coordinates Straw Donations to the Adams Campaigns*

30. I know from my review of review of records from the New York Campaign Finance Board that on or about December 10, 2020, [REDACTED] and four other individuals donated by check approximately \$2,000 each to the 2021 Adams Campaign. Based on my review of the donors' contribution cards, I have learned the following, in substance and in part:

- a. Four of the donors—all except [REDACTED] list their employer as "[REDACTED]" [REDACTED] lists his employer as "Self," with his occupation as "President," lists an email address with a [REDACTED].com domain name, and lists the same employer address as the other individuals. I therefore believe that [REDACTED] was the President of [REDACTED] and the other four donors worked for him. This pattern of donations is materially similar to the

█████ donations discussed above, which I have confirmed, through admissions of the donors and other evidence, were straw donations. (*See* Ex. A at ¶¶ 10-19, Ex. B at ¶¶ 8-10).

b. All five of the contribution cards have matching, pre-typed information, including the recipient and the names and addresses of the respective donors and their employers. Based on my experience reviewing contribution cards, from which I have observed that contribution cards are often filled in by hand, and the use of pre-typed cards is unusual.

c. Because the donations were made on the same day in matching amounts by employees of the same organization using substantially similar contribution cards, I believe they were coordinated.

31. Based on my review of █████ bank records, I have learned that in or about December 2020—around the time █████ donated \$2,000 to the 2021 Adams Campaign—█████ received a number of deposits to the same bank account in the approximate amount of \$2,000 to \$3,000. While I am not at this time able to identify any specific deposit as a reimbursement for █████ donation, and such a reimbursement may not have occurred, these deposits are also consistent with such a reimbursement.

32. Another of the donors described in Paragraph 30 is █████ who is listed on his contribution card as a Project Manager for █████ Based on my review of █████ bank records, a check from █████ account to the 2021 Adams Campaign for approximately \$2,000 is dated on or about December 10, 2020, and cleared on or about December 22, 2020. Also on or December 10 and 21, 2020, █████ account received two cash deposits totaling approximately \$2,000. Accordingly, █████ received approximately \$2,000 in cash at approximately the same time he gave approximately \$2,000 to the 2021 Adams Campaign.

33. I also know from my review of records from the New York Campaign Finance Board that on or about June 13 and 14, 2023, [REDACTED] and six other individuals, among others, donated to the 2025 Adams Campaign as follows:

Name	Amount
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000

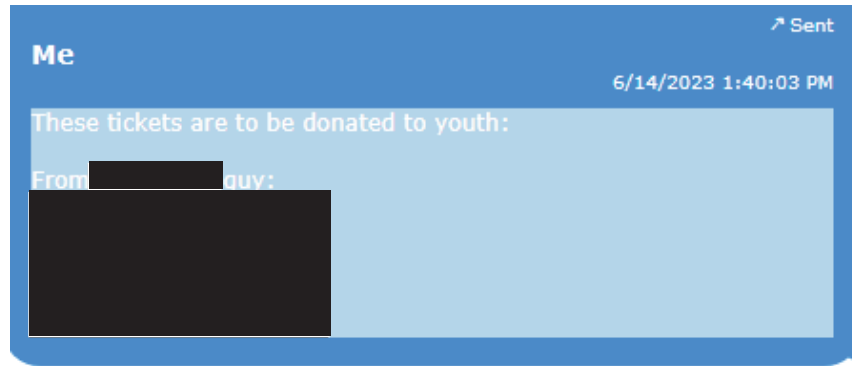
34. Public reporting states that the 2025 Adams Campaign hosted a fundraiser on Broadway on or about June 16, 2023.¹²

35. Based on my review of messages obtained from an electronic devices belonging to

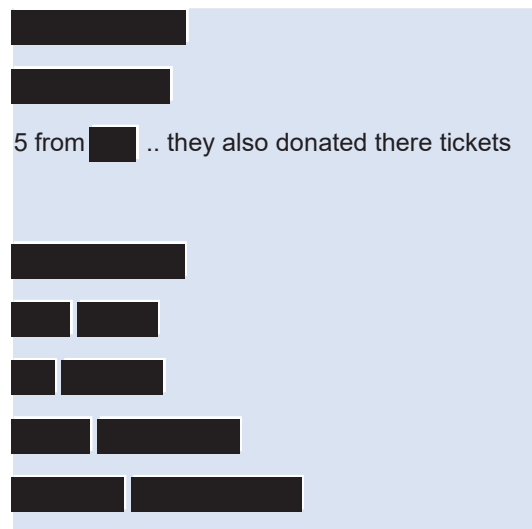
[REDACTED] obtained pursuant to a search warrant, I have learned the following:

a. On or about June 14, 2023, [REDACTED] sent the following message:

¹² See <https://www.cityandstateny.com/politics/2023/06/eric-adams-fundraising-broadway-show-new-york-new-york/387039/>.



b. On or about June 16, 2023, [redacted] received a message from a phone number identified as "[redacted]". [redacted] is likely [redacted] who I know from my participation in this investigation is a senior advisor to Adams for South Asian and Muslim Affairs. The message to [redacted] states:



The seven names in this message are the same seven names identified as donors to the 2025 Adams Campaign in Paragraph 33.

c. Based on the above messages, I believe that [redacted] coordinated five of the donations, including his own donation, and that all of the donors donated their tickets rather than attend the Broadway fundraiser.

36. Based on my review of materials obtained from [REDACTED] electronic devices pursuant to a search warrant, I have learned that on or about October 10, 2023, [REDACTED] sent a message to the [REDACTED] Phone stating, in substance and in part, “This is [REDACTED] Mayor Adams’ fundraiser. I’m reaching out regarding scheduling a fundraiser, can you please give me a call back when you have a moment?” That phone number appears in [REDACTED] Apple Contacts as the number for “[REDACTED],” and the organization is listed as “Uzbek/ Brooklyn.”

[REDACTED] Appears to Have Separately Engaged in Money Laundering Activity

37. Based on my review of bank records, I have learned the following:

- a. Along with another individual (“Individual-1”), who also donated to the 2021 Adams Campaign as an employee of [REDACTED] as discussed above, [REDACTED] is a signatory for a bank account in the name of [REDACTED]
- b. On or about January 24, 2020, [REDACTED] received a wire in the amount of approximately \$11.7 million from [REDACTED] a Cyprus-based entity.
- c. Approximately three days later, [REDACTED] wired approximately \$11.7 million to another bank account, also in the name of [REDACTED] and also for which [REDACTED] and Individual-1 were signatories.
- d. Approximately three days later, [REDACTED] wired approximately \$11.7 million in two transfers to two bank accounts. Approximately \$11.5 million were transferred to an account in the name of [REDACTED] ending in 3167 (the “3167 [REDACTED] Account”), and for which [REDACTED] and Individual-1 were signatories. The remaining approximately \$200,000 were transferred to another account in the name of [REDACTED] this one ending in 8865 (the “8865 [REDACTED] Account”), and for which [REDACTED] and Individual-1 were signatories.

e. Approximately one week later, on February 6, 2020, [REDACTED] wired approximately \$11.5 million from the 3167 [REDACTED] Account to the 8865 [REDACTED] Account.

f. The same day, on or about February 6, 2020, the 8865 [REDACTED] Account wired approximately \$11.7 million to a company called [REDACTED]

38. Based on my review of New York City real estate records, I have learned that on or about February 7, 2020, [REDACTED] purchased a building in Brooklyn, New York, for approximately \$13 million.

39. Based on my participation in money laundering investigations, I know that the rapid movement of large sums of money between accounts, as described above, is indicative of an effort to conceal or disguise the nature and source of the funds.

B. Probable Cause Regarding the Subject Account

40. I have reviewed records from the Provider showing that the Subject Account is registered to [REDACTED]

41. Furthermore, based on records obtained from the Provider, I know that the Subject Account contains, *inter alia*, iCloud backups, calendars, photos, contact lists, messages, notes, and iCloud drive information. I also know from my experience in this case searching other iCloud accounts that such accounts can contain communications exchanged on encrypted applications such as WhatsApp and Signal, even if that cannot be discerned from the records I currently possess. As set forth above, [REDACTED] has received at least one electronic message from [REDACTED] regarding fundraising efforts for the Adams Campaigns.

42. Also as set forth above, [REDACTED] made phone calls to city officials, [REDACTED] Adams, and an Uzbek official. I know from my experience that records of those calls, contact information

for those officials, and electronic communications associated with arranging or following up on those calls may be present in iCloud accounts like the Subject Account.

43. Further, as set forth above, [REDACTED] posted on photos on social media concerning his relationship with Adams, his efforts to influence the city government, and his relationships with the Uzbek government. I know from my experience that those photos, and other similar photos, may be present on the Subject Account.

44. For the reasons detailed above, I submit that there is probable cause to believe that evidence of communications concerning the contribution of funds under the names of donors other than the true donor, some of which may have obtained matching funds for which they were not eligible, evidence of money laundering, and other evidence of the Subject Offenses described in Section II of Attachment A to the proposed warrant are likely to be found in the Subject Account.

45. Temporal Limitation: This application is limited to all content created, sent, received, accessed, modified, or deleted on or after January 1, 2020, the same month as the money laundering activity described above and the same year as the 2020 straw donations described above.

C. Evidence, Fruits and Instrumentalities

46. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Providers' servers associated with the Subject Account will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

III. Review of the Information Obtained Pursuant to the Warrant

47. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement

personnel within 7 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

48. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

49. The existence and general nature of this investigation are publicly known, because of media reporting, and are known to certain subjects and targets such as Adams and [REDACTED] including because of the execution of various warrants. However, the scope, exact nature of this ongoing

criminal investigation and the particular types of evidence the Government is covertly seeking as part of that investigation are not publicly known, and specifically, this investigation's interest on [REDACTED] is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets to as-yet non-public information about the nature and scope of the Government's investigation, which could cause them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. Indeed, the targets of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. *See* 18 U.S.C. § 2705(b)(3).

50. Accordingly, there is reason to believe that, were the Provider to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of one year from issuance, subject to extension upon application to the Court, if necessary.

51. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.


V. Conclusion

52. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C.

§ 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

s/ [REDACTED] by the Court with permission
SA [REDACTED]
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, this
5th day of April, 2024



Honorable Robyn F. Tarnofsky
United States Magistrate Judge
Southern District of New York

09.20.2021

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

24 MAG 1398

In the Matter of a Warrant for All
Content and Other Information
Associated with the iCloud Account
Associated with [REDACTED] bk.ru,
Maintained at Premises Controlled by
Apple Inc., USAO Reference No.
2021R00778

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Apple Inc. ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent [REDACTED] of the FBI, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the iCloud account associated with [REDACTED] bk.ru, maintained at premises controlled by the Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 7 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 7 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or

tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

April 5, 2024
Date Issued

3:11 PM
Time Issued



UNITED STATES MAGISTRATE JUDGE
Southern District of New York

iCloud Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Apple Inc. (the “Provider”), headquartered at 1 Infinite Loop, Cupertino, California 95014, and applies to all content and other information within the Provider’s possession, custody, or control associated with the iCloud account [REDACTED]bk.ru (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from January 1, 2018 through the date of this Warrant and Order, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from January 1, 2018 through the date of this Warrant and Order, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of: (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same), and (iv) 18 U.S.C. § 1956 (money laundering and conspiracy to commit money laundering) for content created, sent, received, accessed, modified, or deleted on or after January 1, 2020, including the following:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Account.
2. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 New York City Mayoral campaign of Eric Adams (the “2021 Adams Campaign”) on the part of any donor or associate of any donor; the Government of Uzbekistan; or the 2021 Adams Campaign.
3. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2025 New York City Mayoral campaign of Eric Adams (the “2025 Adams Campaign,” and together with the 2021 Adams Campaign, the “Adams Campaigns”) on the part of any donor or associate of any donor; the Government of Uzbekistan; or the 2025 Adams Campaign.
4. Evidence relating to coordination between Uzbek nationals or the Uzbek Government and the Adams Campaigns concerning political contributions to the Adams Campaigns, including,

but not limited to, evidence of motive and intent for Uzbek nationals or the Uzbek Government to provide or facilitate campaign contributions to the Adams Campaigns, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaigns to provide benefits, whether lawfully or unlawfully, to Uzbek nationals or the Uzbek Government in return for campaign contributions.

5. Evidence relating to payments to employees, officers, and associates of [REDACTED] [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaigns.

6. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] for campaign contributions to the Adams Campaigns.

7. Evidence relating to the source of funds for payment or reimbursement of persons serving as conduits for campaign contributions to the Adams Campaigns originating from Uzbek nationals.

8. Evidence of individuals or entities who donated to the Adams Campaigns before or after receiving transfers of funds similar to the amount of the donation.

9. Evidence regarding straw donations to the Adams Campaigns, including without limitation evidence regarding the identities of any persons or entities involved, wittingly or unwittingly, in straw donations, and evidence regarding the sources of funds for straw donations.

10. Evidence of the relationship between and among (i) persons or entities that coordinated or made straw donations or (ii) foreign nationals and/or governments, and any person who is or was associated with or employed by the Adams Campaigns, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

11. Evidence of an intent to exchange benefits between the Uzbek Government or entities and persons acting at its behest, and any person who is or was associated with or employed by the Adams Campaigns, including but not limited to straw donations and any actions taken by any person who is or was associated with or employed by the Adams Campaigns on behalf of the Uzbek Government, [REDACTED] or other entities associated with [REDACTED]

12. Evidence of an effort to transfer funds in order to hide the true origin and source of those funds, including evidence of an intent to hide the nature of such funds, and including evidence of any unlawful activity that was the original source of such funds.

13. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Subject Account.

14. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

15. Evidence concerning efforts to conceal communications, meetings, or associations between Uzbek nationals or [REDACTED] and persons associated with or employed by the Adams Campaigns.

16. Evidence concerning efforts to destroy or conceal evidence of the Subject Offenses or to devise or coordinate false exculpatory explanations for the conduct underlying the Subject Offenses, or to otherwise obstruct law enforcement from investigating the Subject Offenses.

EXHIBIT A
[22 MAG 9730]